

Claims

What is claimed is:

- 1 1. A method, comprising:
 - 2 issuing, via a caller computer, a request to have a firmware service be
 - 3 performed via firmware on a remote computer
 - 4 authenticating the caller computer; and
 - 5 performing the firmware service if the caller computer is authenticated,
 - 6 otherwise denying access to the firmware service.
- 1 2. The method of claim 1, further comprising initializing a listening mechanism
- 2 on the remote computer to receive the request.
- 1 3. The method of claim 2, wherein the listening mechanism is interrupt-based,
- 2 further comprising asserting an interrupt on a processor of the remote computer in
- 3 response to receiving the request.
- 1 4. The method of claim 2, wherein the listening mechanism is polling-based,
- 2 further comprising periodically polling a network interface of the remote computer to
- 3 determine if the remote computer has received a request.

1 5. The method of claim 1, wherein the caller computer is authenticated by
2 performing operations including:
3 issuing an authentication challenge to the caller computer; and
4 evaluating a response by the caller computer to the authentication challenge.

1 6. The method of claim 5, wherein the operations further include:
2 encrypting original data using a first key held by the remote computer to
3 create encrypted original data;
4 sending the encrypted original data to the calling computer;
5 decrypting the encrypted original data using a second key held by the caller
6 computer to create decrypted data;
7 sending the decrypted data back to the remote computer;
8 comparing the decrypted data with the original data to authenticate the calling
9 computer.

1 7. The method of claim 6, further comprising extracting the first key from an
2 authentication certificate for the caller computer issued to the remote computer.

1 8. The method of claim 7, wherein the first key is an public key contained in the
2 authentication certificate and the second key comprises a private key held by the
3 calling computer that is the asymmetric key for the public key.

1 9. The method of claim 1, further comprising:

2 issuing at least one authentication certificate to the remote computer, each of
3 said at least one authentication certificate containing authentication information
4 corresponding to a respective caller computer;
5 receiving authentication credentials from a caller computer;
6 authenticating the caller computer via the authentication credentials in view of
7 a corresponding authentication certificate from among said at least one
8 authentication certificate issued to the remote computer.

1 10. The method of claim 9, further comprising determining if an authentication
2 certificate corresponding to the caller computer has expired.

1 11. The method of claim 9, further comprising determining if an authentication
2 certificate corresponding to the caller computer has been revoked.

1 12. The method of claim 1, further comprising authenticating the remote
2 computer.

1 13. The method of claim 1, further comprising sending encrypted traffic relating to
2 the firmware service request and results of the request between the caller computer
3 and the remote computer.

1 14. The method of claim 13, further comprising performing a cipher negotiation
2 between the caller computer and the remote computer to agree upon an encryption
3 technique used to encrypt and decrypt the encrypted traffic.

1 15. The method of claim 14, wherein the encryption technique employs at least
2 one session key.

1 16. The method of claim 1, wherein communications between the caller computer
2 and the remote computer are performed using an out-of-band communication
3 channel that operates independent of an operating system to run or running on the
4 remote computer.

1 17. An article of manufacture, comprising:
2 a machine-readable medium on which a plurality of instructions are stored,
3 which when executed perform operations comprising:
4 receive a request from a caller computer to perform a firmware service;
5 authenticate the caller computer; and
6 perform the firmware service if the caller computer is authenticated,
7 otherwise denying access to the firmware service.

1 18. The article of manufacture of claim 17, wherein execution of the plurality of
2 instructions further performs the operation of initializing a listening mechanism to
3 receive the request.

1 19. The article of manufacture of claim 17, wherein execution of the plurality of
2 instructions further performs operations including:

3 issuing an authentication challenge to the caller computer;
4 receiving a response to the authentication challenge from the caller computer;
5 and
6 evaluating the response to determine whether the caller computer is
7 authenticate.

1 20. The article of manufacture of claim 19, wherein evaluating the response to the
2 authentication challenge comprises:

3 extracting authentication credentials for the caller computer contained in the
4 response;
5 identifying an authentication certificate corresponding to the caller computer;
6 and
7 checking authentication credentials for the caller computer against the
8 authentication certificate that is identified.

1 21. The article of manufacture of claim 20, wherein execution of the plurality of
2 instructions further performs the operation of determining if the authentication
3 certificate that is identified has expired.

1 22. The article of manufacture of claim 20, wherein execution of the plurality of
2 instructions further performs the operation of determining if the authentication
3 certificate that is identified has been revoked.

1 23. The article of manufacture of claim 19, wherein execution of the plurality of
2 instructions performs further operations including:

3 generating a random number;
4 encrypting the random number using a first key to create an encrypted
5 random number;
6 sending the encrypted random number to the calling computer;
7 receiving decrypted data derived from the encrypted random number from the
8 calling computer
9 comparing the decrypted data with the random number to authenticate the
10 calling computer.

1 24. The article of manufacture of claim 17, wherein the article comprises a
2 firmware storage device and the plurality of instructions comprise firmware.

1 25. The article of manufacture of claim 17, wherein execution of the plurality of
2 instructions further performs the operation of performing a cipher negotiation
3 between the caller computer and a remote computer on which the plurality of
4 instructions are executed to agree upon an encryption technique to be used to

5 encrypt and decrypt encrypted traffic to be sent between the caller computer and the
6 remote computer.

1 26. The article of manufacture of claim 25, wherein the encryption technique
2 employs a shared asymmetric session key.

1 27. A computer system, comprising:
2 a processor;
3 a memory, operatively coupled to the processor;
4 a network interface operatively coupled to the processor; and
5 at least one flash device operatively coupled to the processor on which
6 firmware instructions are stored, which when executed by the processor perform
7 operations comprising:
8 receive a request to perform a firmware service received from a caller
9 computer via the network interface;
10 authenticate the caller computer; and
11 perform the firmware service if the caller computer is authenticated,
12 otherwise denying access to the firmware service

1 28. The computer system of claim 27, wherein execution of the firmware
2 instructions performs the further operation of periodically polling the network
3 interface to determine if the network interface has received a request from a caller
4 computer to perform a firmware service.

1 29. The computer system of claim 27, wherein execution of the firmware
2 instructions performs further operations, including:
3 issuing an authentication challenge to the caller computer;
4 receiving a response to the authentication challenge from the caller computer;
5 and
6 evaluating the response to determine whether the caller computer is
7 authenticate.

1 30. The computer system of claim 27, wherein execution of the firmware
2 instructions further performs the operation of performing a cipher negotiation
3 between the caller computer and the computer system to agree upon an encryption
4 technique to be used to encrypt and decrypt encrypted traffic to be sent between the
5 caller computer and the computer system.